(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
23 septembre 2004 (23.09.2004)

PCT

(10) Numéro de publication internationale
WO 2004/082286 A1

(51) Classification internationale des brevets[7] : H04N 7/167

(21) Numéro de la demande internationale : PCT/EP2004/050299

(22) Date de dépôt international : 12 mars 2004 (12.03.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
03/50044 12 mars 2003 (12.03.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : CANAL+ TECHNOLOGIES [FR/FR]; 34 Place Raoul Dautry, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : DAUVOIS, Jean-Luc [FR/FR]; 19 rue Eugène Manuel, F-75116 Paris (FR). CASSAGNE, Philippe [FR/FR]; 18 rue du Bourg Tibourg, F-75004 Paris (FR).

(74) Mandataire : WEIHS, Bruno; Osha Novak & May, 121 avenue des Champs Elysées, F-75008 Paris (FR).

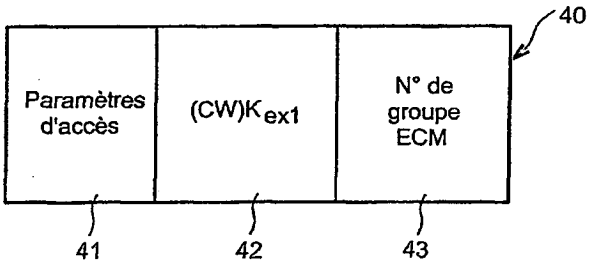
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Suite sur la page suivante]

(54) Title: PAY TELEVISION SYSTEM, METHOD FOR TRANSMISSION OF SCRAMBLED AUDIOVISUAL PROGRAMMES, DECODER AND CHIP FOR CARRYING OUT SAID METHOD

(54) Titre : SYSTEME DE TELEVISION A PEAGE, PROCEDE DE DIFFUSION DE PROGRAMMES AUDIOVISUELS BROUILLES, DECODEUR ET CARTE A PUCE METTANT EN OEUVRE CE PROCEDE



41... ACCESS PARAMETERS
43... NUMBER OF THE ECM GROUP

(57) Abstract: The invention relates to a method for broadcasting a scrambled audiovisual programme to decoders (11), comprising a step for transmission of first messages (ECM) to said decoders, each comprising a control word (CW), encrypted using a operation key permitting each decoder to unscramble the received audiovisual programme during a given period, second messages (EMM) comprising operation keys according to which during the same basic period as the scrambling time for the scrambled audiovisual programme, there is transmission of at least two first messages, each containing the same control word respectively encrypted by distinct operation keys and second messages, each containing one of said operation keys and an individual or group address of at least one decoder of the at least two decoder units.

(57) Abrégé : La présente invention concerne un procédé de diffusion d'un programme audiovisuel brouillé à destination de décodeurs (11) comprenant une étape d'émission vers ces décodeurs de premiers messages (ECM) contenant chacun un mot de contrôle (CW) crypté par une clé d'exploitation, pour permettre à chaque décodeur de désembrouiller, durant une période de temps donnée, le programme audiovisuel reçu, de seconds messages (EMM) comprenant des clés d'exploitation, selon lequel au cours de l'étape d'émission, pour une même période élémentaire de temps de brouillage du programme audiovisuel brouillé, il y a émission d'au moins deux premiers messages comprenant chacun un même mot de contrôle crypté par des clés d'exploitation distinctes respectives, et de seconds messages qui contiennent chacun l'une de ces clés d'exploitation ainsi qu'une adresse, individuelle ou de groupe, d'au moins un décodeur de l'un d'au moins deux ensembles de décodeurs.

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

SYSTEME DE TELEVISION A PEAGE, PROCEDE DE DIFFUSION DE PROGRAMMES AUDIOVISUELS BROUILLES, DECODEUR ET CARTE A PUCE METTANT EN ŒUVRE CE PROCEDE

DESCRIPTION

DOMAINE TECHNIQUE

La présente invention concerne un système de télévision à péage, un procédé de diffusion de programmes audiovisuels brouillés, un décodeur et une carte à puce mettant en œuvre ce procédé. L'invention a pour objet des procédé, système, décodeur et carte qui visent à limiter, notamment en réaction à la détection d'une action malveillante, l'impact frauduleux que peut avoir cette action, en terme de piratage, sur un parc de décodeurs dans un système de télévision à péage. Plus précisément, l'action frauduleuse consiste en la révélation totalement illicite de clés.

ETAT DE LA TECHNIQUE ANTERIEURE

Les techniques utilisées en télévision payante, comme décrit par exemple dans l'article intitulé « Functional model for a conditional access system » (EBU Technical Review, 1995, n°266, pages 64 à 77), sont basées sur deux mécanismes indépendants : d'une part sur un brouillage du (ou des) programme(s) vidéo et/ou audio (ci-après « programme audiovisuel »), d'autre part sur une fonction d'allocation de clés et droits commerciaux qui sont transmis, typiquement comme des messages d'accès conditionnels (EMM et ECM) sécurisés cryptés au boîtier de désembrouillage ou au décodeur, ou à la carte qui lui est associée à travers

le décodeur. Le brouillage peut être appliqué sur un flot de bits numérique définissant le programme audiovisuel.

Le programme audiovisuel transmis brouillé en utilisant des clés, ne peut être désembrouillé qu'en utilisant des équivalents de ces clés, appelés mots de contrôle (CW). A noter qu'une distinction est faite dans la présente description par utilisation des mots « brouiller/désembrouiller » et « crypter/décrypter » selon qu'ils s'appliquent à un programme audiovisuel ou à des messages d'accès conditionnels, respectivement. Pour chaque programme audiovisuel, les valeurs de mot de contrôle transmis vers les décodeurs changent périodiquement à une fréquence relativement élevée, par exemple de l'ordre de la seconde. Pour permettre le désembrouillage en réception d'un programme audiovisuel, des messages ECM de contrôle d'allocation de droits ("Entitlement Control Messages") et des messages EMM de gestion d'allocation de droits ("Entitlement Management Messages") sont transmis vers les décodeurs.

Ces deux types de messages ECM et EMM peuvent être envoyés, au travers du décodeur, à une carte à puce ou tout objet portable, tel qu'une carte PCMCIA (« personal computer memory card international association » ou « association internationale de carte à mémoire à ordinateur personnel »), une clé à puce..., qui assure notamment des fonctions de décryptage et de stockage de droits d'utilisateur. Dans la présente description le terme « carte » désigne tout objet

portable fonctionnant en relation avec le décodeur, typiquement en étant logé dans un lecteur du décodeur.

Les messages ECM contiennent des mots de contrôle cryptés, ces mots de contrôle permettant au décodeur de désembrouiller un programme audiovisuel. Les messages ECM sont transmis à la carte qui décrypte les mots de contrôle cryptés et envoie au décodeur ces mots de contrôle CW. La carte ne réalise l'opération de décryptage des mots de contrôle cryptés que si l'utilisateur est autorisé à accéder au programme audiovisuel en cours. Pour cela la carte mémorise dans une zone de sa mémoire les droits alloué à l'utilisateur concerné. Ainsi, lorsqu'un utilisateur est associé par abonnement à une carte à puce, l'autorisation d'accès est indiquée par des données d'allocation de droits ("entitlement data") mémorisées dans la carte.

Les messages EMM contiennent des informations qui permettent de mettre à jour les données d'allocation de droits de l'utilisateur, par exemple en modifiant les données mémorisées dans la carte. Dans le cas d'une offre de prévisualisation désembrouillée temporaire et selon la technique antérieure, un premier message EMM est envoyé au décodeur pour offrir à l'abonné temporairement les droits requis pour accéder à un programme sur un canal donné. A défaut de transaction de paiement reçu par le système de gestion des droits de l'Opérateur, un autre message EMM est envoyé pour révoquer ces mêmes droits.

Il est à noter que le démultiplexage entre les messages EMM et ECM reçus est typiquement réalisé

par le décodeur en fonction d'informations issues d'une table indiquant les flux MPEG (identifiés par des valeurs de « Packet Identifier Data ») véhiculant les différents types respectifs de messages. Le filtrage des messages EMM portant une adresse de groupe ou l'adresse unique du décodeur est également opéré avantageusement par le décodeur.

Les messages ECM et EMM peuvent comprendre un champ de signature numérique qui assure l'intégrité du message (par exemple un code de Hash). Ceci permet de détecter toute corruption malveillante ou accidentelle des contenus des messages.

Un message ECM est émis avec le programme brouillé. Il comprend typiquement au moins deux champs. Le premier champ comprend les paramètres d'accès, qui définissent les conditions sous lesquelles l'accès aux programmes est autorisé. Ce champ permet par exemple un contrôle parental (Un code PIN additionnel peut être requis avant de donner accès au programme désembrouillé). Le second champ de chaque message ECM contient un mot de contrôle, noté CW, sous forme cryptée par une clé dite d'exploitation ou de service. Ce mot de contrôle qui change à une fréquence relativement élevée, typiquement de l'ordre de la seconde, permet le désembrouillage d'un programme audiovisuel.

Un message EMM comprend avantageusement au moins trois champs. Un premier champ d'adresse permet d'adresser un décodeur individuel ou un groupe de décodeurs pour lui/leur transmettre les informations véhiculées par les autres champs EMM. Un second champ

contient les autorisations d'accès aux programmes pour les abonnés. Un troisième champ contient une clé d'exploitation cryptée. La valeur prise par cette clé d'exploitation varie à une fréquence relativement faible, par exemple de l'ordre de plusieurs jours ou du mois . Selon la technique antérieure, pour une période de temps donné, cette clé d'exploitation est la même pour l'ensemble du parc d'abonnés considéré.

Typiquement selon la technique antérieure, un message EMM donné d'envoi de clé d'exploitation contient l'adresse d'un décodeur unique, ou d'un groupe de décodeurs, et la clé d'exploitation préalablement cryptée par une clé propre et unique à la carte à puce du décodeur ou du groupe de décodeurs considéré.

Les messages EMM peuvent aussi être utilisés pour envoyer une commande au décodeur. L'émission de messages EMM est généralement le résultat d'une action (abonnement) ou d'un défaut d'action (non paiement en mode "Pay-Par-View" avec prévisualisation désembrouillé temporaire) de l'utilisateur à l'Opérateur. Ces messages EMM sont en général individuels. Leur contenu est interprété par le décodeur (ou la carte associée) ou par un nombre limité des décodeurs qui sont concernés par ces droits particuliers. Les messages EMM ne sont pas émis de façon synchrone avec le programme audiovisuel auquel ils s'appliquent. Ils sont transmis à l'avance afin de permettre l'accès à un programme donné d'un utilisateur autorisé. N'importe quel réseau peut être utilisé pour transmettre ces messages EMM au récepteur : modem, courrier ou radiodiffusion. Avantageusement, par

contre, chaque message ECM est pour sa part transmis avec une très légère avance temporelle, mais de manière quasi-synchrone, par rapport à la portion de programme audiovisuel qu'il est destiné à désembrouiller, pour prendre en compte le temps de décryptage du mot de contrôle qu'il contient sous forme cryptée.

Pour être sûr qu'un message EMM a été reçu par l'utilisateur, pour renouveler une souscription par exemple, celui-ci est envoyé plusieurs fois. Les messages EMM sont ainsi organisés cycliquement selon une période donnée pour l'émission. La durée d'une telle période définit le temps maximum à attendre pour obtenir une allocation de droit pour un utilisateur qui a coupé son décodeur pendant une longue durée.

Le fait que selon la technique antérieure, pour une période de temps donné, la clé d'exploitation est la même pour l'ensemble d'un parc d'abonnés considéré, tout en étant cryptée par des clés uniques respectives différentes selon les décodeurs auxquels ladite clé d'exploitation est destinée, pose un problème évident de sécurité dans le cas ou cette clé d'exploitation est révélée.

L'invention a pour objet de réduire au minimum l'impact que peut avoir la découverte par un pirate de clés d'exploitation, utilisées dans les systèmes audiovisuels. Selon des techniques de piratage connues, une personne malveillante, ou pirate, ayant découvert une clé d'exploitation peut mettre celle-ci à disposition des tiers afin qu'ils puissent ainsi décrypter les messages ECM pour recouvrer les mots de contrôle et ainsi désembrouiller le (les) programme(s)

audiovisuels brouillés diffusés par les Opérateurs. Le pirate met alors à disposition des tiers utilisateurs les clés d'exploitation décryptées, chacune de ces clés d'exploitation restant « valable » pour une durée relativement longue (de l'ordre de plusieurs jours) pour décrypter les mots de contrôle CW, qui permettent de désembrouiller le programme brouillé. Cette mise à disposition s'effectue par exemple par utilisation d'un site Internet. Les tiers peuvent alors se connecter à ce site Internet totalement illicite, dit « pirate », et venir lire périodiquement les clés requises pour permettre le désembrouillage de programmes audiovisuels brouillés afin de programmer frauduleusement leurs décodeurs et/ou cartes d'abonné.

L'invention a pour objet de remédier a posteriori à ce type de problème, dès lors qu'il est découvert qu'une ou des clés d'exploitation sont frauduleusement mises à la disposition de tiers.

EXPOSÉ DE L'INVENTION

La présente invention propose donc un procédé de diffusion d'un programme audiovisuel brouillé à destination de décodeurs comprenant des étapes :

- d'émission vers ces décodeurs de premiers messages contenant chacun un mot de contrôle crypté par une clé d'exploitation pour permettre à chaque décodeur de désembrouiller, durant une période de temps donnée, le programme audiovisuel reçu, et de seconds messages comprenant des clés d'exploitation,

caractérisé en ce que au cours de l'étape d'émission, pour une même période élémentaire de temps de brouillage du programme audiovisuel brouillé, il y a émission d'au moins deux premiers messages comprenant chacun un même mot de contrôle crypté par des clés d'exploitation distinctes respectives, et de seconds messages qui contiennent chacun l'une de ces clés d'exploitation ainsi qu'une adresse, individuelle ou de groupe, d'au moins un décodeur de l'un d'au moins deux ensembles de décodeurs pour permettre le décryptage, par les décodeurs de chaque ensemble, de ce même mot de contrôle crypté par ces clés d'exploitation distinctes respectives.

Ainsi, l'impact en terme de fraude de la divulguation frauduleuse d'une clé d'exploitation est limité à un groupe de l'ensemble du parc d'aboné.

Avantageusement, chaque premier message comprend un champ d'adresse de groupe apte à être traité par chaque décodeur, ou par la carte qui lui est associée, pour filtrer les seuls premiers messages correspondant à l'adresse de celui-ci.

Avantageusement, ledit procédé comprend des étapes :

a) de transmission, en cas de divulgation frauduleuse de l'une des clés d'exploitation, dans des seconds messages en mode d'adressage groupé à destination du groupe de décodeurs utilisant ladite clé d'exploitation divulguée frauduleusement, de nouvelles clés d'exploitation respectives à destination de sous-groupes dudit groupe,

b) de transmission, en cas de nouvelle divulgation frauduleuse de l'une des nouvelle clés d'exploitation, dans des seconds messages en mode d'adressage groupé à destination d'un sous-groupe de décodeurs utilisant ladite nouvelle clé d'exploitation divulguée frauduleusement, de nouvelles clés respectives à des sous-sous-groupes de ce sous-groupe,

c) de réitération de l'étape b) à chaque nouvelle divulgation frauduleuse d'une nouvelle clé d'exploitation.

L'invention concerne également un système de télévision à péage comprenant une système de contrôle d'accés et une liaison par satellite, terrestre ou par câble entre ce système et les décodeurs d'au moins deux abonnés, caractérisé en ce que ces décodeurs forment au moins deux ensembles distincts, et en ce que chaque décodeur comprend des moyens de filtrage des premiers messages en fonction de l'adresse du décodeur ou de la carte qui lui est associée.

L'invention concerne, également, une carte à puce, ou un décodeur, qui comprend des moyens pour filtrer les premiers messages en fonction de l'adresse du décodeur ou de la carte qui lui est associée.

BRÈVE DESCRIPTION DES DESSINS

La figure 1 illustre un système d'émission de télévision à péage de l'art connu fonctionnant dans le domaine de la télévision numérique ;

La figure 2 illustre le contenu d'un message EMM,

La figure 3 illustre un exemple de réalisation d'un système d'autorisation d'abonnés ;

La figure 4 illustre un champ d'adresse d'un message EMM dans un exemple de réalisation de l'invention ;

La figure 5 illustre un message ECM dans une variante de l'invention.

EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

Comme illustré sur la figure 1, un système de contrôle d'accès, selon un mode de réalisation non limitatif, comprend un système de gestion d'abonné (SMS ou « Subscriber Management System ») 9 relié à un système d'autorisation d'abonné (SAS ou « Subscriber Autorisation System ») 10. Il est supposé, aux seules fins de simplification de la description qui suit, qu'un seul programme audiovisuel est transmis.

Ce système d'autorisation d'abonné 10 ainsi qu'un générateur de mot de contrôle (CW) 11 sont reliés à une station d'émission d'opérateur 12, chacun via un circuit de cryptage 13 et 14. Le circuit de cryptage 13 crypte chaque message EMM non crypté reçu par une clé dite unique propre au décodeur, ou à la carte associée, auquel le message EMM considéré est destiné, cela

typiquement en fonction de l'adresse véhiculée par l'un des champs de chaque message EMM. Le signal appliqué par le système d'autorisation d'abonné 10 à une entrée du circuit de cryptage 14 véhicule des clés d'exploitation successives qui sont utilisées par le circuit de cryptage 14 pour crypter les mots de contrôle CW générés par le générateur 11. Le choix par le circuit de cryptage 14 de la clé d'exploitation qui doit être utilisée pour crypter les mots de contrôle CW générés par le générateur 11 dépend d'un champ de numéro de groupe ECM, ce champ étant lui-même défini par le circuit de cryptage 14 en fonction du nombre de clés d'exploitation disponibles à un instant donné, telles que reçues du système 10. Le champ de numéro de groupe ECM sera décrit plus en détails dans la suite de la description.

Cette station d'émission d'opérateur 12 reçoit des signaux image I, son S et éventuellement données D qui transitent successivement au travers d'un multiplexeur 15, d'un brouilleur 16, d'un modulateur 17 et d'un émetteur 18.

Le système de gestion d'abonné 9, dans un exemple de réalisation, comprend une base de données d'abonnés, qui, pour chaque abonné, comporte en particulier le nom, le prénom, la formule d'abonnement choisi (qui définit les programmes auxquels l'abonné peut avoir accès) et le numéro de la carte à puce. Cette base de données est mise à jour à chaque nouvel abonnement ou chaque résiliation d'abonnement.

Le système d'autorisation d'abonnés 10 est responsable de la génération des messages EMM. Chaque

message EMM, dans un exemple de réalisation préféré, comprend, au moins un champ d'adresse 20, un champ de droits d'accès 21, un champ de clé d'exploitation Sk 22, et un champ de vérification d'intégrité par exemple par champ de fonction de Hash 23, comme représenté sur la figure 2.

Un tel message EMM, et notamment la clé Sk, est crypté, au moins partiellement, par une clé dite unique, qui correspond à une clé de la carte à puce, à laquelle le message est destiné par adressage au moyen du champ d'adresse. Le contenu d'un tel message EMM est renouvelé périodiquement, par exemple tous les mois, pour changer la clé Sk, utilisée pour décrypter les messages ECM.

Comme illustré sur la figure 3, le système d'autorisation d'abonnés 10, peut comprendre :

- un module de génération de clé 30,
- un module d'adressage 31,
- un module de génération de code Hash 32,
- un multiplexeur 33.

Un signal de communication COM est appliqué sur des entrées respectives des modules de génération de clé 30 et d'adressage 31. Des informations de droits d'accès DA sont entrées sur le module de génération de code de Hash 32 et sur le multiplexeur 33.

Le module de génération de code Hash 32 reçoit en entrée des sorties respectives du module de génération de clé 30, du module d'adressage 31, et les informations de droit d'accès DA en provenance du système de gestion d'abonné 9 pour produire un code Hash pour chaque message EMM.

Des sorties du module de génération de clé 30, du module de génération de code Hash 32, et du module d'adressage 31 ainsi que les informations de droit d'accès DA sont appliquées au multiplexeur 33, qui produit les messages EMM successifs non cryptés par clé unique.

Selon l'invention, dès lors que la divulgation frauduleuse d'une clé d'exploitation pour un groupe d'abonné donné, par exemple par consultation d'un site Internet, est détectée, une commande COM est appliquée à des entrées respectives du module de génération de clé 30 et du module d'adressage 31 afin que :

(a) d'une part, le module de génération de clé 30, qui générait jusqu'à cet instant une seule clé pour ce groupe d'abonné donné, génère désormais ou à partir d'un instant ultérieur donné, en réponse à la réception de la commande COM, au moins deux clés, et

(b) d'autre part, qu'en lieu et place d'une seule adresse de groupe d'abonné pour ce groupe d'abonné donné, au moins deux adresses de groupe d'abonnés soient générées par le module d'adressage 31 pour envoyer par adressage les au moins deux clés ainsi générées à ces deux groupes distincts d'abonnés.

Dans les dispositifs de l'art antérieur, une valeur de mot de contrôle CW, destinée à désembrouiller une période élémentaire de temps de brouillage d'un programme audiovisuel brouillé donné, est transmise dans un message ECM en étant cryptée par une seule clé d'exploitation, elle-même transmise sous forme cryptée dans des messages EMM. Cette clé

d'exploitation est transmise vers les décodeurs dans différents messages EMM sous forme cryptée par des clés uniques respectives différentes. Dans le procédé de l'invention, il y a émission d'au moins deux messages ECM (chacun destiné à désembrouiller une même période élémentaire de temps de brouillage d'un programme audiovisuel brouillé) comprenant chacun un même mot de contrôle crypté par des clés d'exploitation distinctes respectives.

Ainsi, dans le procédé de l'invention, pour une période élémentaire de temps de brouillage d'un programme audiovisuel brouillé donné, chaque valeur de mot de contrôle CW donnée est cryptée par au moins deux clés d'exploitation distinctes entre elles avant d'être émise dans des messages ECM respectifs. Les au moins deux clés d'exploitation ainsi utilisées pour le cryptage d'une même valeur de mot de contrôle sont transmises dans des messages EMM respectifs à destination de décodeurs différents, pour permettre l'obtention, par décryptage, de cette même valeur de mot de contrôle par ces décodeurs.

Dans l'invention on utilise la notion de "message EMM de groupe". Un tel message permet d'adresser simultanément plusieurs décodeurs, au moyen d'un seul message EMM, et de transmettre à chacun d'eux la clé d'exploitation qu'ils devront utiliser. Les clés respectives transmises aux différents groupes de décodeurs peuvent être identiques ou différentes entre elles. Chacun des décodeurs d'un groupe considéré possède donc une même clé, dite clé unique, pour

décrypter la clé d'exploitation reçue dans un message EMM en mode d'adressage groupé.

Dans un premier exemple de réalisation de simple illustration, on considère un parc de n décodeurs, par exemple n=4000, adressables par un champ d'adresse du message EMM, par exemple de N = 12 bits (2^{12} = 4096) B1 à B12, comme illustré sur la figure 4. Les 10 bits B3 à B12 servent à adresser un groupe de 1024 (2^{10}) décodeurs tandis que les bits B1 et B2 permettent d'adresser 2^2 = 4 groupes distincts de 1024 décodeurs. Selon que les bits B1 et B2 prennent respectivement les valeurs "00", "01", "10" et "11", quatre groupes distincts de décodeurs peuvent être adressés.

Très avantageusement selon l'invention, on peut rajouter aux messages ECM un champ "numéro de groupe ECM". Les messages ECM 40, comme illustré sur la figure 5, contiennent alors :

- un champ 41 de paramètres d'accès,
- un champ 42 de mode de contrôle,
- un champ 43 de numéro de groupe ECM.

Un tel champ 43 permet, typiquement à la carte à puce ou au décodeur, de filtrer les seuls messages ECM que la carte est capable de décrypter. En effet, cette carte à puce, ou ce décodeur, ne possède pas, en provenance de messages EMM, d'autres clés d'exploitation que la clé d'exploitation K_{exn} (en supposant qu'il y ait une clé unique par décodeur), qui permet de décrypter les mots de contrôle (CW)K_{exn} cryptés par la clé K_{exn}, n étant un nombre entier compris entre 1 et 2^N, N étant le nombre de bits de ce

champ. Il faut remarquer que seuls les messages EMM correspondant au profil d'adresse du décodeur/carte sont effectivement filtrés et traités.

Dans un second exemple de réalisation illustrant plus précisément l'invention, on considère un parc de 800 000 décodeurs définis chacun par une adresse de 20 bits pour pouvoir être tous adressés (2^{20} = 1 048 576). Les 10 bits de poids faibles définissent les adresses des décodeurs au sein d'un groupe. Les 10 bits de poids forts définissent les adresses de groupes de décodeurs. Un message EMM de groupe permet, par exemple, d'adresser simultanément $Q = 2^{10} = 1024$ décodeurs au moyen d'un seul message EMM, pour transmettre à chacun d'eux la clé d'exploitation qu'ils doivent utiliser. 1024 messages EMM de groupe sont envoyés périodiquement, pour adresser l'ensemble des décodeurs du parc.

Dans les dispositifs de l'art connu, ces 1024 messages EMM de groupe transportent une même clé d'exploitation. Cette clé d'exploitation est véhiculée dans un message EMM sous une forme cryptée par une clé, dite unique, différente des clés utilisées pour le cryptage de cette même clé d'exploitation dans les autres 1023 messages EMM. La divulgation frauduleuse de cette seule clé d'exploitation peut entraîner un dommage considérable.

Selon l'invention, dès lors que la révélation frauduleuse d'une clé d'exploitation Kex1 est constatée, on n'utilise plus cette clé d'exploitation révélée frauduleusement Kex1 mais on utilise M clés nouvelles, par exemple deux clés notées

Kex2 et Kex3, M étant un entier typiquement compris en 2 et N. On modifie le contenu des messages EMM de groupe envoyés jusqu'alors périodiquement en incluant dans 512 messages EMM la clé d'exploitation Kex2 respectivement cryptée par 512 clés uniques respectives. On inclut dans les autres 512 messages EMM la clé d'exploitation Kex3 respectivement cryptée par 512 clés uniques respectives. Ainsi, 512 messages EMM de groupe véhiculent de manière cryptée la clé d'exploitation Kex2, et 512 messages EMM de groupe véhiculent de manière cryptée la clé d'exploitation Kex3.

Le contenu des messages ECM véhiculant les mots de contrôle cryptés par les clés d'exploitation est donc modifié du fait de la modification de ces clés d'exploitation utilisées pour le cryptage des mots de contrôle. Pour cela, comme considéré précédemment, on tient compte d'un champ "Numéro de groupe ECM" et on réalise un envoi de messages ECM par adressage de groupe.

L'adressage de groupe dans les messages EMM peut être opéré de la manière suivante. Toutes les adresses de groupes (bits de poids forts exprimés sur 10 bits) "0000000000" à "0111111111" permettent d'adresser la clé d'exploitation K_{ex2} aux 512 premiers groupes de 1024 décodeurs tandis que les adresses de groupes (bits de poids forts exprimés sur 10 bits) "1000000000" à "1111111111" permettent d'adresser la clé d'exploitation K_{ex3} à 512 autres groupes de 1024 décodeurs.

Dans le cas des messages ECM, le positionnement à 1 ou à 0 d'un seul premier bit de poids le plus fort du champ "Numéro de groupe ECM" permet alors à la carte à puce ou au décodeur de filtrer les seuls messages ECM que la carte est capable de décrypter. En effet, la carte ne possède qu'une seule clé d'exploitation (soit la clé d'exploitation K_{ex2}, soit la clé K_{ex3}) en provenance des messages EMM. Cette clé permet de décrypter les mots de contrôle effectivement cryptés par cette même clé ou une clé correpondante (par exemple en mode cryptographique assymétrique).

Si l'on détecte une nouvelle divulgation frauduleuse de l'une ou l'autre des deux clés d'exploitation K_{ex2} ou K_{ex3} on n'utilise plus cette clé d'exploitation, par exemple K_{ex2}, mais on utilise rapidement M nouvelles clés, par exemple quatre clés notées K_{ex4}, K_{ex5}, K_{ex6}, K_{ex7}. La clé non divulguée K_{ex3} continue pour sa part à être utilisée et les messages EMM à adresses de groupe (bits de poids forts exprimés sur 10 bits) allant de "1000000000" à "1111111111" continuent d'adresser la clé d'exploitation K_{ex3} à 512 groupes de 1024 décodeurs. De même, les messages ECM dont le premier bit de poids le plus fort du champ "Numéro de groupe ECM" est positionné à "1" continuent de véhiculer les mots de contrôle cryptés par la clé d'exploitation K_{ex3} à destination des décodeurs.

Par contre, le contenu des messages EMM à adresses de groupe (bits de poids forts exprimés sur 10 bits) allant de "0000000000" à "0111111111" est modifié. Si on utilise ces quatre nouvelles clés de

remplacement K_{ex4}, K_{ex5}, K_{ex6}, K_{ex7} pour remplacer la clé d'exploitation K_{ex2} :

- Toutes les adresses de groupes EMM (bits de poids forts exprimés sur 10 bits) "0000000000" à "0001111111" permettent d'adresser la clé d'exploitation K_{ex4} à 128 sous-groupes de 1024 décodeurs.

- Toutes les adresses de groupes EMM (bits de poids forts exprimés sur 10 bits) "0010000000" à "0011111111" permettent d'adresser la clé d'exploitation K_{ex5} à 128 sous-groupes de 1024 décodeurs.

- Toutes les adresses de groupes EMM (bits de poids forts exprimés sur 10 bits) "0100000000" à "0101111111" permettent d'adresser la clé d'exploitation K_{ex6} à 128 sous-groupes de 1024 décodeurs.

- Toutes les adresses de groupes EMM (bits de poids forts exprimés sur 10 bits) "0110000000" à "0111111111" permettent d'adresser la clé d'exploitation K_{ex7} à 128 sous-groupes de 1024 décodeurs.

Dans le cas des messages ECM, le positionnement à 00, 01, 10, 11 des seuls second et troisième bits de poids les plus fort du champ "Numéro de groupe ECM" permet typiquement à la carte à puce ou au décodeur de filtrer les seuls messages ECM que la carte est capable de décrypter. En effet, une carte donnée ne possède en provenance des messages EMM qu'une seule clé d'exploitation (l'une des clés K_{ex4}, K_{ex5}, K_{ex6} ou K_{ex7}) permettant de décrypter les mots de contrôle

cryptés par l'une de ces clés ou une clé correspondante (par exemple en mode cryptographique.assymétrique)..

A l'issue de cette étape, on a donc 5 clés d'exploitation différentes véhiculées sous forme cryptée à savoir K_{ex3}, K_{ex4}, K_{ex5}, K_{ex6} ou K_{ex7}.

On réitère les étapes décrites ci-dessus à chaque fois que l'on détecte une divulgation frauduleuse de l'une des clés d'exploitation existant alors, jusqu'à potentiellement réduire à néant l'impact de la révélation frauduleuse de clés par le détenteur d'un décodeur puisqu'il sera, dans une hypothèse théorique finale poussée à l'extrême, le seul à utiliser la clé d'exploitation divulguée frauduleusement. On peut même identifier à partir de l'adresse générée par l'unité 10 (figure 3) pour cette clé d'exploitation, le décodeur (ou plus précisément la carte associée et donc l'abonné) à l'origine de la divulguation frauduleuse de clés. La mise en œuvre de l'invention pourra néanmoins se limiter à réduire l'impact potentiel que pourrait avoir la révélation frauduleuses d'une clé d'exploitation à un groupe limité d'abonné mais toutefois substantiel, car en effet, la réduction à l'extrême (un seul décodeur) du nombre de décodeurs utilisant la même clé d'exploitation a pour contrepartie d'augmenter considérablement la taille du champ "Numéro de groupe ECM" de messages ECM, et le nombre de messages ECM à transmettre ou diffuser. Or les messages ECM sont émis à fréquence très élevée, ce qui alors a pour conséquence une implication très importante sur la

bande passante requise. Il s'agit ici donc d'un choix de mise en oeuvre en fonction :

- de la bande passante que l'on souhaite allouer aux messages ECM, et
- du niveau de réduction de nuissance que l'on souhaite mettre en oeuvre par rapport à la divulgation frauduleuse de clés d'exploitation.

REVENDICATIONS

1. Procédé de diffusion d'un programme audiovisuel brouillé à destination de décodeurs (11) comprenant une étape d'émission vers ces décodeurs de premiers messages (ECM) contenant chacun un mot de contrôle (CW) crypté par une clé d'exploitation, pour permettre à chaque décodeur de désembrouiller, durant une période de temps donnée, le programme audiovisuel reçu, et de seconds messages (EMM) comprenant des clés d'exploitation,
caractérisé en ce que au cours de l'étape d'émission, pour une même période élémentaire de temps de brouillage du programme audiovisuel brouillé, il y a émission d'au moins deux premiers messages (ECM) comprenant chacun un même mot de contrôle crypté par des clés d'exploitation distinctes respectives, et de seconds messages (EMM) qui contiennent chacun l'une de ces clés d'exploitation ainsi qu'une adresse, individuelle ou de groupe, d'au moins un décodeur de l'un d'au moins deux ensembles de décodeurs pour permettre le décryptage, par les décodeurs de chaque ensemble, de ce même mot de contrôle crypté par ces clés d'exploitation distinctes respectives.

2. Procédé selon la revendication 1, dans lequel chaque premier message (ECM) comprend un champ d'adresse de groupe apte à être traité par chaque décodeur, ou par la carte qui lui est associée, pour filtrer les seuls premiers messages (ECM) correspondant à l'adresse de celui-ci.

3. Procédé selon la revendication 1 ou 2, comprenant des étapes :

a) de transmission, dans le cas d'une divulgation frauduleuse de l'une des clés d'exploitation, dans des seconds messages (EMM) en mode d'adressage groupé à destination du groupe de décodeurs utilisant ladite clé d'exploitation divulguée frauduleusement, de nouvelles clés d'exploitation respectives à destination de sous-groupes dudit groupe,

b) de transmission, dans le cas d'une nouvelle divulgation frauduleuse de l'une des nouvelles clés d'exploitation, dans des seconds messages (EMM) en mode d'adressage groupé à destination d'un sous-groupe de décodeurs utilisant ladite nouvelle clé d'exploitation divulguée frauduleusement, de nouvelles clés respectives à des sous-sous-groupes correspondant à ce sous-groupe,

c) de réitération de l'étape b) à chaque nouvelle divulgation frauduleuse d'une nouvelle clé d'exploitation.

4. Système de télévision à péage comprenant un système de contrôle d'accès et une liaison (32) entre celui-ci et les décodeurs d'au moins deux abonnés, caractérisé en ce que les décodeurs forment au moins deux ensembles distincts, et en ce que chaque décodeur comprend des moyens de filtrage de premiers messages (ECM) en fonction de l'adresse du décodeur.

5. Carte à puce pour traiter des premiers messages transmis selon l'une quelconque des revendications 2 et 3, lorsque cette dernière dépend de la revendication 2, caractérisée en ce qu'elle comprend des moyens pour filtrer les premiers messages (ECM) en fonction de l'adresse du décodeur ou de ladite carte à puce.

6. Décodeur pour traiter des premiers messages transmis selon l'une quelconque des revendications 2 et 3 lorsque cette dernière dépend de la revendication 2, caractérisé en ce qu'il comprend des moyens pour filtrer les premiers messages (ECM) en fonction de l'adresse du décodeur ou de ladite carte à puce.

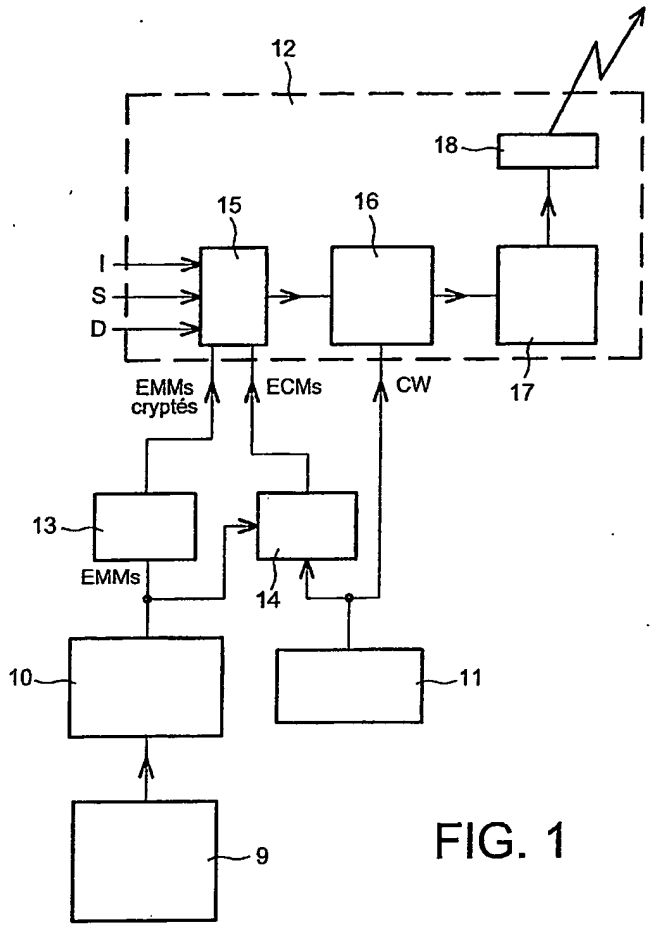


FIG. 1

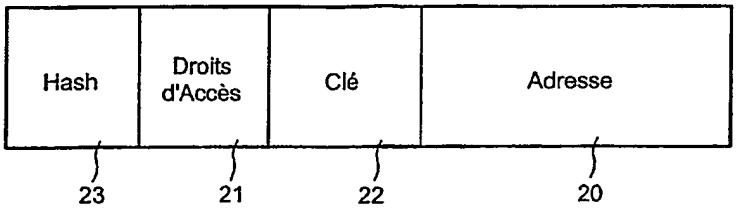

Hash
Droits d'Accès
Clé
Adresse
23
21
22
20

FIG. 2

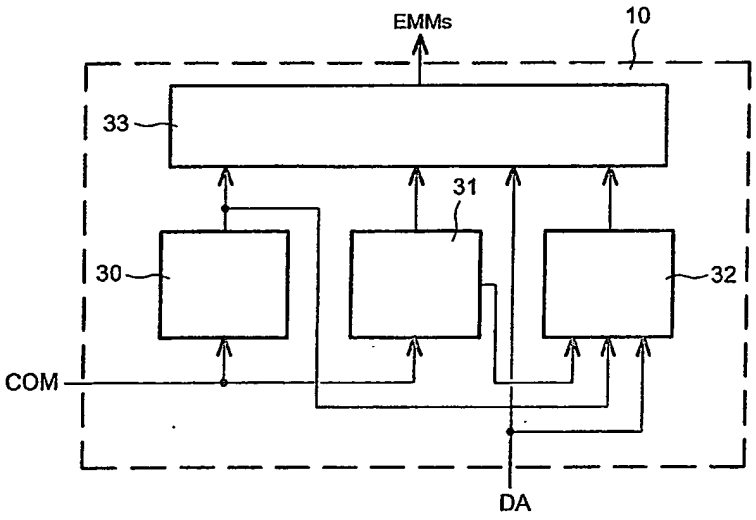

EMMs
10
33
31
30
32
COM
DA

FIG. 3

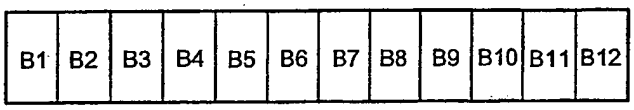

B1
B2
B3
B4
B5
B6
B7
B8
B9
B10
B11
B12

FIG. 4

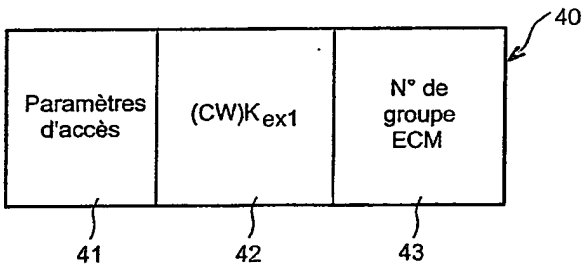

40
Paramètres d'accès
(CW)K ex1
N° de groupe ECM
41
42
43

FIG. 5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/050299

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 111 923 A (IRDETO ACCESS BV) 27 June 2001 (2001-06-27) paragraph '0003!	1-6
Y	FR 2 825 877 A (CANAL PLUS TECHNOLOGIES) 13 December 2002 (2002-12-13) page 2, line 26 - page 5, line 20	1-6
A	US 5 748 732 A (LE BERRE JACQUES ET AL) 5 May 1998 (1998-05-05) column 3, line 58 - column 4, line 8	1-6
A	WO 00/04718 A (BENARDEAU CHRISTIAN ; CANAL PLUS SA (FR); DAUVOIS JEAN LUC (FR)) 27 January 2000 (2000-01-27) page 20, line 21 - page 22, line 3	1-6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 July 2004	26/07/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bertrand, F

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/050299

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99/09743 A (SCIENTIFIC ATLANTA) 25 February 1999 (1999-02-25) the whole document	1-6
A	EP 0 817 485 A (THOMSON MULTIMEDIA SA) 7 January 1998 (1998-01-07) the whole document	1-6

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/050299

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1111923 A	27-06-2001	EP 1111923 A1	27-06-2001
		AU 4049501 A	03-07-2001
		BR 0008324 A	29-01-2002
		CA 2364398 A1	28-06-2001
		CN 1357197 T	03-07-2002
		WO 0147271 A2	28-06-2001
		EP 1238537 A2	11-09-2002
		HU 0200126 A2	29-05-2002
		JP 2003518843 T	10-06-2003
		NZ 513568 A	28-11-2003
		TW 554627 B	21-09-2003
		US 2002126847 A1	12-09-2002
		ZA 200106073 A	19-12-2002
FR 2825877 A	13-12-2002	FR 2825877 A1	13-12-2002
		CA 2450186 A1	19-12-2002
		EP 1421789 A1	26-05-2004
		WO 02102074 A1	19-12-2002
US 5748732 A	05-05-1998	FR 2730372 A1	09-08-1996
		DE 69610343 D1	26-10-2000
		DE 69610343 T2	29-03-2001
		EP 0726676 A1	14-08-1996
		JP 8251569 A	27-09-1996
WO 0004718 A	27-01-2000	AT 226379 T	15-11-2002
		AU 755892 B2	02-01-2003
		AU 4642599 A	07-02-2000
		BR 9912091 A	03-04-2001
		CA 2337066 A1	27-01-2000
		CN 1317203 T	10-10-2001
		DE 69903557 D1	21-11-2002
		DE 69903557 T2	26-06-2003
		EP 1099348 A1	16-05-2001
		ES 2185365 T3	16-04-2003
		HK 1033518 A1	11-09-2003
		HR 20010033 A1	28-02-2002
		HU 0301694 A2	29-09-2003
		WO 0004718 A1	27-01-2000
		ID 27161 A	08-03-2001
		JP 2002521879 T	16-07-2002
		NO 20010227 A	15-03-2001
		NZ 509760 A	28-08-2002
		PL 345531 A1	17-12-2001
		TR 200100571 T2	23-07-2001
		ZA 200100325 A	11-01-2002
WO 9909743 A	25-02-1999	US 6157719 A	05-12-2000
		AU 1581699 A	08-03-1999
		AU 8670598 A	22-02-1999
		AU 8679798 A	22-02-1999
		AU 8679898 A	22-02-1999
		AU 8764298 A	22-02-1999
		AU 8823398 A	22-02-1999
		AU 8823698 A	22-02-1999
		BR 9810966 A	20-11-2001
		BR 9810967 A	30-10-2001
		BR 9810971 A	13-04-2004

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/050299

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9909743 A		BR 9815606 A	22-01-2002
		BR 9815607 A	13-11-2001
		BR 9815610 A	22-06-2004
		DE 69802288 D1	06-12-2001
		DE 69802288 T2	27-06-2002
		DE 69802540 D1	20-12-2001
		DE 69802540 T2	23-05-2002
		DE 69808113 D1	24-10-2002
		DE 69808113 T2	22-05-2003
		DE 69809757 D1	09-01-2003
		DE 69809757 T2	10-07-2003
		EP 1193974 A2	03-04-2002
		EP 1189438 A2	20-03-2002
		EP 1189439 A2	20-03-2002
		EP 1010323 A1	21-06-2000
		EP 1010324 A1	21-06-2000
		EP 1010325 A1	21-06-2000
		EP 1013091 A1	28-06-2000
		EP 1000508 A1	17-05-2000
		EP 1000509 A1	17-05-2000
		EP 1000511 A2	17-05-2000
		JP 2001513587 T	04-09-2001
		JP 2002506296 T	26-02-2002
		JP 2003522425 T	22-07-2003
		JP 2003521818 T	15-07-2003
		JP 2003521718 T	15-07-2003
		JP 2001512842 T	28-08-2001
		JP 2003521820 T	15-07-2003
		WO 9907145 A1	11-02-1999
		WO 9907146 A1	11-02-1999
		WO 9907147 A1	11-02-1999
		WO 9907148 A1	11-02-1999
		WO 9907149 A1	11-02-1999
		WO 9909743 A2	25-02-1999
		WO 9907150 A1	11-02-1999
		US 6105134 A	15-08-2000
		US 2003074565 A1	17-04-2003
		US 2003169879 A1	11-09-2003
		US 6424717 B1	23-07-2002
EP 0817485 A	07-01-1998	FR 2750554 A1	02-01-1998
		CN 1171015 A ,B	21-01-1998
		DE 69715535 D1	24-10-2002
		DE 69715535 T2	22-05-2003
		EP 0817485 A1	07-01-1998
		JP 10164052 A	19-06-1998
		US 6035038 A	07-03-2000

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/EP2004/050299

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/167

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 1 111 923 A (IRDETO ACCESS BV) 27 juin 2001 (2001-06-27) alinéa '0003!	1-6
Y	FR 2 825 877 A (CANAL PLUS TECHNOLOGIES) 13 décembre 2002 (2002-12-13) page 2, ligne 26 - page 5, ligne 20	1-6
A	US 5 748 732 A (LE BERRE JACQUES ET AL) 5 mai 1998 (1998-05-05) colonne 3, ligne 58 - colonne 4, ligne 8	1-6
A	WO 00/04718 A (BENARDEAU CHRISTIAN ; CANAL PLUS SA (FR); DAUVOIS JEAN LUC (FR)) 27 janvier 2000 (2000-01-27) page 20, ligne 21 - page 22, ligne 3	1-6

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
14 juillet 2004	26/07/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bertrand, F

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/EP2004/050299

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 99/09743 A (SCIENTIFIC ATLANTA) 25 février 1999 (1999-02-25) le document en entier	1-6
A	EP 0 817 485 A (THOMSON MULTIMEDIA SA) 7 janvier 1998 (1998-01-07) le document en entier	1-6

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/EP2004/050299

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 1111923	A	27-06-2001	EP	1111923 A1	27-06-2001
			AU	4049501 A	03-07-2001
			BR	0008324 A	29-01-2002
			CA	2364398 A1	28-06-2001
			CN	1357197 T	03-07-2002
			WO	0147271 A2	28-06-2001
			EP	1238537 A2	11-09-2002
			HU	0200126 A2	29-05-2002
			JP	2003518843 T	10-06-2003
			NZ	513568 A	28-11-2003
			TW	554627 B	21-09-2003
			US	2002126847 A1	12-09-2002
			ZA	200106073 A	19-12-2002
FR 2825877	A	13-12-2002	FR	2825877 A1	13-12-2002
			CA	2450186 A1	19-12-2002
			EP	1421789 A1	26-05-2004
			WO	02102074 A1	19-12-2002
US 5748732	A	05-05-1998	FR	2730372 A1	09-08-1996
			DE	69610343 D1	26-10-2000
			DE	69610343 T2	29-03-2001
			EP	0726676 A1	14-08-1996
			JP	8251569 A	27-09-1996
WO 0004718	A	27-01-2000	AT	226379 T	15-11-2002
			AU	755892 B2	02-01-2003
			AU	4642599 A	07-02-2000
			BR	9912091 A	03-04-2001
			CA	2337066 A1	27-01-2000
			CN	1317203 T	10-10-2001
			DE	69903557 D1	21-11-2002
			DE	69903557 T2	26-06-2003
			EP	1099348 A1	16-05-2001
			ES	2185365 T3	16-04-2003
			HK	1033518 A1	11-09-2003
			HR	20010033 A1	28-02-2002
			HU	0301694 A2	29-09-2003
			WO	0004718 A1	27-01-2000
			ID	27161 A	08-03-2001
			JP	2002521879 T	16-07-2002
			NO	20010227 A	15-03-2001
			NZ	509760 A	28-08-2002
			PL	345531 A1	17-12-2001
			TR	200100571 T2	23-07-2001
			ZA	200100325 A	11-01-2002
WO 9909743	A	25-02-1999	US	6157719 A	05-12-2000
			AU	1581699 A	08-03-1999
			AU	8670598 A	22-02-1999
			AU	8679798 A	22-02-1999
			AU	8679898 A	22-02-1999
			AU	8764298 A	22-02-1999
			AU	8823398 A	22-02-1999
			AU	8823698 A	22-02-1999
			BR	9810966 A	20-11-2001
			BR	9810967 A	30-10-2001
			BR	9810971 A	13-04-2004

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/EP2004/050299

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9909743 A		BR 9815606 A	22-01-2002
		BR 9815607 A	13-11-2001
		BR 9815610 A	22-06-2004
		DE 69802288 D1	06-12-2001
		DE 69802288 T2	27-06-2002
		DE 69802540 D1	20-12-2001
		DE 69802540 T2	23-05-2002
		DE 69808113 D1	24-10-2002
		DE 69808113 T2	22-05-2003
		DE 69809757 D1	09-01-2003
		DE 69809757 T2	10-07-2003
		EP 1193974 A2	03-04-2002
		EP 1189438 A2	20-03-2002
		EP 1189439 A2	20-03-2002
		EP 1010323 A1	21-06-2000
		EP 1010324 A1	21-06-2000
		EP 1010325 A1	21-06-2000
		EP 1013091 A1	28-06-2000
		EP 1000508 A1	17-05-2000
		EP 1000509 A1	17-05-2000
		EP 1000511 A2	17-05-2000
		JP 2001513587 T	04-09-2001
		JP 2002506296 T	26-02-2002
		JP 2003522425 T	22-07-2003
		JP 2003521818 T	15-07-2003
		JP 2003521718 T	15-07-2003
		JP 2001512842 T	28-08-2001
		JP 2003521820 T	15-07-2003
		WO 9907145 A1	11-02-1999
		WO 9907146 A1	11-02-1999
		WO 9907147 A1	11-02-1999
		WO 9907148 A1	11-02-1999
		WO 9907149 A1	11-02-1999
		WO 9909743 A2	25-02-1999
		WO 9907150 A1	11-02-1999
		US 6105134 A	15-08-2000
		US 2003074565 A1	17-04-2003
		US 2003169879 A1	11-09-2003
		US 6424717 B1	23-07-2002
EP 0817485 A	07-01-1998	FR 2750554 A1	02-01-1998
		CN 1171015 A ,B	21-01-1998
		DE 69715535 D1	24-10-2002
		DE 69715535 T2	22-05-2003
		EP 0817485 A1	07-01-1998
		JP 10164052 A	19-06-1998
		US 6035038 A	07-03-2000

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☑ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.